
The Background Screening Credentialing Council volunteer members drafted the following response to questions about Information Security in Clause 1.1 of the BSAAP Standard, version 2.0, effective April 6, 2018. This letter is an informal discussion of the question posed and does not constitute a legal opinion of the BSCC.

TITLE: Clause 1.1 - Information Security – PII and SOC 2 (Type II) Audit Criteria

Issue: My company is in the preparations stages for seeking for accreditation. Our IT Security Manager, has a question about the first standard. We hold our PII data at a hosted data center that meets the SOC 2 (Type II), will this be enough to satisfy this criterion?

Response: The current Background Screening Agency Accreditation Program's (hereafter "Accreditation Program") Accreditation Standard with Audit Criteria, effective as of April 6, 2018, provides as follows in Clause 1.1 with respect to Information Security:

> ***1.1 Information Security Certification***
> *Wherever Personally Identifiable Information (PII) is held, whether at CRA, CRA's data center (whether internal or hosted), an/or CRA's platform provider (whether internal or hosted) such entity must hold a current (current as defined by the certifying body) information security certification and/or provide written evidence of completing an information security audit for which no critical, high-risk, or severe security vulnerabilities remain uncured. The source of such certification and/or written evidence must be a qualified security assessor.*

In the Attributes of and Suggestions for Onsite Audit (What auditor will look for in policy, procedure, activity), the Audit Criteria go on to provide specifically:

> *Wherever Personally Identifiable Information (PII) is held, whether at CRA, CRA's data center (whether internal or hosted), and/or CRA's platform provider (whether internal or hosted) such entity must hold a current (current as defined by the certifying body) information security certification or written evidence of information security audit by a qualified security assessor for which no critical, high-risk, or severe security vulnerabilities remain uncured. Examples of acceptable certifications/audits include [sic] but are not limited to: 1) ISO 27001:2013, 2) SOC 2 (Type II), 3) EI3PA, 4) NIST SP 800-37 and NIST SP 800-53 rev 4, and PCI. Alternatively, written evidence of audits will be acceptable if: 1) certification document is provided, 2) audit results signed by auditor show no critical, high-risk, or severe security vulnerabilities remain uncured, or 3) signed attestation from auditor including date of audit, name of qualified security assessor, name of auditing company, statement that no critical, high-risk, or critical security vulnerabilities remain uncured, and 4) name of security standard/s used as basis for auditing.*

Thus, holding your PII data (from a digital standpoint) at a data center that holds a current an active SOC II (Type II) certification, does satisfy Clause 1.1 of Accreditation Standard 2.0.

We do think it is important to note that in addition to satisfying Clause 1.1. re: Information Security Certification, accredited agencies must also satisfy the rest of the clauses surrounding Information Security and set forth in Clauses 1.2 through 1.12. Together, these clauses set forth requirements for a comprehensive Information Security policy that includes appropriate data access, storage, backup, security, masking, destruction and related information security practices.

In conclusion, it is our view that having PII hosted at an off-site data center that holds the SOC 2 (Type II) certification will satisfy Clause 1.1 of the Accreditation Standard 2.0. However, satisfying clause 1.1. in and of itself not be enough to fully satisfy all of the Information Security standards and audit criteria set forth in Accreditation Standard 2.0. The standard and the audit criteria go well beyond the hosting of PII and further require a more comprehensive information security policy that addresses the full scope of the items indicated above.

Thank you for submitting your question and allowing us to respond in a manner that is beneficial to all applicants. We believe we have responded fully to your inquiry. Please let us know if you have any further questions.